# Методология классификации угроз нарушения информационной безопасности

Конев Антон Александрович
Зам. директора Института системной интеграции и безопасности ТУСУР

# Methodology for classifying information security threats

Konev Anton
Deputy Director of the ISIB TUSUR

# ВМЕСТО АКТУАЛЬНОСТИ

ТУСУР
TUSUR UNIVERSITY

**Обеспечение информационной безопасности организации** – деятельность, направленная на *устранение (нейтрализацию, парирование) внутренних и внешних угроз* информационной безопасности организации или на минимизацию ущерба от возможной реализации таких угроз.

**Объект защиты информации** – *информация* или *носитель информации*, или *информационный процесс*, которые необходимо защищать в соответствии с целью защиты информации.

**Безопасность информации (при применении информационных технологий)** – состояние защищённости информационной технологии, обеспечивающее безопасность информации, для обработки которой она применяется, и информационную безопасность *автоматизированной информационной системы*, в которой она реализована.

# ОГРАНИЧЕНИЯ НА МЕТОДОЛОГИЮ

ТУСУР
TUSUR UNIVERSITY

Подходы к моделированию угроз:

- **на основе описания ресурсов системы и процессов их обработки**;
- на основе описания атак на систему;
- на основе описания структуры системы и её уязвимостей.

Не рассматриваются:

- преднамеренность реализации угрозы;
- модель нарушителя.

# ТРЕБОВАНИЯ К МЕТОДОЛОГИИ КЛАССИФИКАЦИИ УГРОЗ

ТУСУР
TUSUR UNIVERSITY

- Учёт методов функционального (на основе рассмотрения информационных процессов, как объектов защиты) и структурного (на основе рассмотрения автоматизированных информационных систем, как объектов защиты) моделирования.
- Разделение угроз на непересекающиеся классы (одна и та же угроза не может быть включена в разные классы).
- Каждая типовая угроза должна быть применима к объектам защиты и в физической среде, и в киберпространстве.
- Классификация угроз должна учитывать модель CIA (включать угрозы конфиденциальности, целостности и доступности).

# ФУНКЦИОНАЛЬНАЯ МОДЕЛЬ ПРОЦЕССА ОПЛАТЫ ПОКУПКИ ЧЕРЕЗ ТЕРМИНАЛ

# ПРИМЕРЫ УГРОЗ БЕЗОПАСНОСТИ ПРОЦЕССА ОПЛАТЫ ПОКУПКИ

ТУСУР
TUSUR UNIVERSITY

| Элемент | Угрозы конфиденциальности | Угрозы целостности | Угрозы доступности |
|---|---|---|---|
| Угрозы, направленные на информацию и её носители | | | |
| База данных АБС | НСД к базе данных | Уничтожение базы данных | Отказ в обслуживании |
| Реквизиты банковской карты | Перехват данных | Некорректное считывание из-за помех | Блокировка из-за повреждения банковской карты |
| Запрос к АБС | Анализ сетевого трафика | Человек посередине (подмена запроса) | Распределённый отказ в обслуживании |
| Сумма покупки | Общедоступно | Фальсификация | Блокировка из-за повреждения POS-терминала |
| Чек | «Сбор мусора» | Уничтожение | Блокировка из-за повреждения POS-терминала |
| Угрозы, направленные на компоненты системы | | | |
| POS-терминал | Раскрытие настроек системы | Сбой оборудования | - |
| АБС | Сканирование портов и уязвимостей | Подмена доверенного объекта сети | - |
| Угрозы, направленные на компоненты управления системой | | | |
| Алгоритм работы АБС | Раскрытие алгоритмов работы системы защиты | Внедрение НДВ при разработке программного обеспечения | - |
| Структура запроса | Общедоступно | Ошибки в процессе разработки | - |

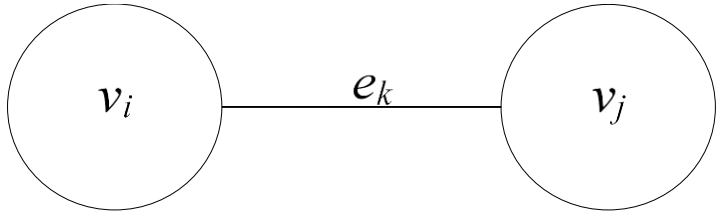
# ПРИНЦИПЫ СТРУКТУРНОГО МОДЕЛИРОВАНИЯ УГРОЗ

ТУСУР
TUSUR UNIVERSITY

- Структура объекта защиты описывается в виде графа, включающего информационные потоки (*информационный поток* – процесс взаимодействия источника информации и ее получателя).
- Источником и получателем информации могут быть как субъекты, так и объекты (*объект* – пассивный компонент системы, хранящий, принимающий или передающий информацию; *субъект* – активный компонент системы, обычно представленный в виде пользователя, процесса или устройства, которые могут явиться причинами потока информации от объекта к объекту или изменения состояния системы).
- Элементарный информационный поток включает в себя три элемента: источник информации, среду распространения и приемник информации.
- Подход к классификации угроз на основе структурного моделирования базируется на операциях над графом – угроза считается реализованной, когда граф претерпевает несанкционированные изменения.

# ЭЛЕМЕНТАРНЫЙ ИНФОРМАЦИОННЫЙ ПОТОК

ТУСУР
TUSUR UNIVERSITY




Описание информационного потока в виде графа:

$f = (v_i, e_k, v_j)$,

где $v_i$, $v_j$ – потенциальные носители защищаемой информации (источник и приемник информации),

$e_k$ – возможная среда распространения защищаемой информации,

$i = 1..n$,

$j = 1..n$,

$k = 1..m$.

Таким образом, можно ввести следующие обозначения множеств:

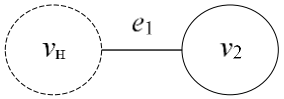
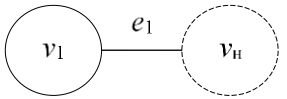
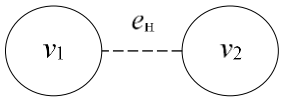
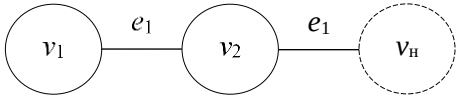
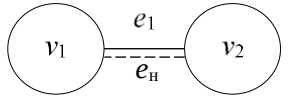
$V = \{v_1, v_2, v_3, ..., v_n\}$ – множество носителей информации;

$E = \{e_1, e_2, e_3, ..., e_m\}$ – множество сред распространения информации (все рассматриваемые среды распространения информации – санкционированные).

# ПРИМЕРЫ УГРОЗ ПРИ СТРУКТУРНОМ МОДЕЛИРОВАНИИ

ТУСУР
TUSUR UNIVERSITY

## Угрозы, направленные на несанкционированное изменение структуры графа

| Угроза | Компьютер ($v_1$) | Сервер БД ($v_2$) | VPN-протокол ($e_1$) |
|---|---|---|---|
| Подмена доверенного объекта сети / использование незащищенного протокола |   |   |   |
| Внедрение в сеть несанкционированного объекта / установка несанкционированного протокола |   | |   |

## Угрозы безопасности информации, возникающие после изменения структуры графа

| | Компьютер ($v_1$) | Сервер БД ($v_2$) | VPN-протокол ($e_1$) |
|---|---|---|---|
| Угрозы конфиденциальности | Несанкционированное считывание файлов | Несанкционированное считывание БД | Перехват сетевого трафика |
| Угрозы целостности | Несанкционированное изменение файлов | Несанкционированное изменение БД | Нарушение целостности сетевых пакетов |

## Угрозы, способные привести к изменению структуры графа при ее санкционированном изменении

| | Компьютер ($v_1$) | Сервер БД ($v_2$) | VPN-протокол ($e_1$) |
|---|---|---|---|
| Угрозы при обновлении или восстановлении работоспособности | Внедрение обновления с вредоносным кодом | Подмена резервной копии конфигурации СУБД | Отсутствие обновления уязвимой версии протокола |
| Угрозы при добавлении нового компонента | Предоставление удаленного доступа с нарушением правил безопасности | Нарушение правил антивирусной защиты при внесении новых данных | Внедрение протокола с недекларированными возможностями |

# ЭЛЕМЕНТЫ МОДЕЛИ ИНФОРМАЦИОННЫХ ПОТОКОВ

ТУСУР
TUSUR UNIVERSITY

В рамках данной работы под **носителем** будут пониматься объекты, способные долговременно хранить информацию (объекты) и ее обрабатывать (субъекты). Под **средой распространения** будут пониматься объекты, предназначенные для осуществления доступа к информации, передачи информации и ее кратковременного хранения во время обработки субъектами.

Таким образом, **носителями** информации **в физической среде** являются:

- человек (субъект);
- физический документ на бумажном носителе, на носителе аналоговой аудио- и видеоинформации и т.п. (объект).

**Носителями** информации **в киберпространстве** являются:

- процесс (субъект);
- файл, база данных и др. (объект).

# ЭЛЕМЕНТЫ МОДЕЛИ ИНФОРМАЦИОННЫХ ПОТОКОВ


Подмножества множества носителей информации $V$:

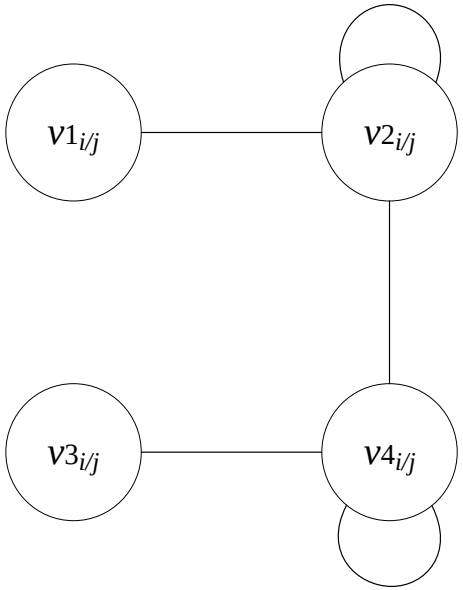
$V1 = \{v1_1, v1_2, v1_3, \ldots, v_{n1}\}$ – подмножество объектов в физической среде (элементы множества – бумажные документы и пр.);

$V2 = \{v2_1, v2_2, v2_3, \ldots, v_{n2}\}$ – подмножество субъектов физической среде (элементы множества – сотрудники, пользователи и пр.);

$V3 = \{v3_1, v3_2, v3_3, \ldots, v_{n3}\}$ – подмножество объектов в киберпространстве (элементы множества – файлы, базы данных и пр.);

$V4 = \{v4_1, v4_2, v4_3, \ldots, v_{n4}\}$ – подмножество субъектов в киберпространстве (элементы множества – системные и прикладные процессы).

# БАЗОВАЯ МОДЕЛЬ ИНФОРМАЦИОННЫХ ПОТОКОВ




| | $v1_j$ | $v2_j$ | $v3_j$ | $v4_j$ |
|---|---|---|---|---|
| $v1_i$ | 0 | 1 | 0 | 0 |
| $v2_i$ | 1 | 1 | 0 | 1 |
| $v3_i$ | 0 | 0 | 0 | 1 |
| $v4_i$ | 0 | 1 | 1 | 1 |

| Приемник / Источник | $v1_j$ | $v2_j$ | $v3_j$ | $v4_j$ |
|---|---|---|---|---|
| $v1_i$ | - | Чтение документа | - | - |
| $v2_i$ | Редактирование документа | Переговоры | - | Ввод информации в компьютер |
| $v3_i$ | - | - | - | Считывание информации из файла |
| $v4_i$ | - | Вывод информации компьютером | Запись информации в файл | Межпроцессное взаимодействие |

# СРЕДЫ РАСПРОСТРАНЕНИЯ ИНФОРМАЦИИ

ТУСУР
TUSUR UNIVERSITY

Подмножества множества сред распространения информации $E$:

$E1 = \{e1_1, e1_2, e1_3, \ldots, e1_{m1}\}$ – подмножество сред распространения акустической информации;

$E2 = \{e2_1, e2_2, e2_3, \ldots, e2_{m2}\}$ – подмножество сред распространения визуальной информации (физического доступа);

$E3 = \{e3_1, e3_2, e3_3, \ldots, e3_{m3}\}$ – подмножество сред распространения информации в виде сигналов;

$E4 = \{e4_1, e4_2, e4_3, \ldots, e4_{m4}\}$ – подмножество сред распространения информации в киберпространстве;

$E2r = \{e2r_1, e2r_2, e2r_3, \ldots, e2r_{m2r}\}$ – подмножество сред дистанционного распространения визуальной информации;

$E3r = \{e3r_1, e3r_2, e3r_3, \ldots, e3r_{m3r}\}$ – подмножество сред дистанционного распространения информации в виде сигналов;

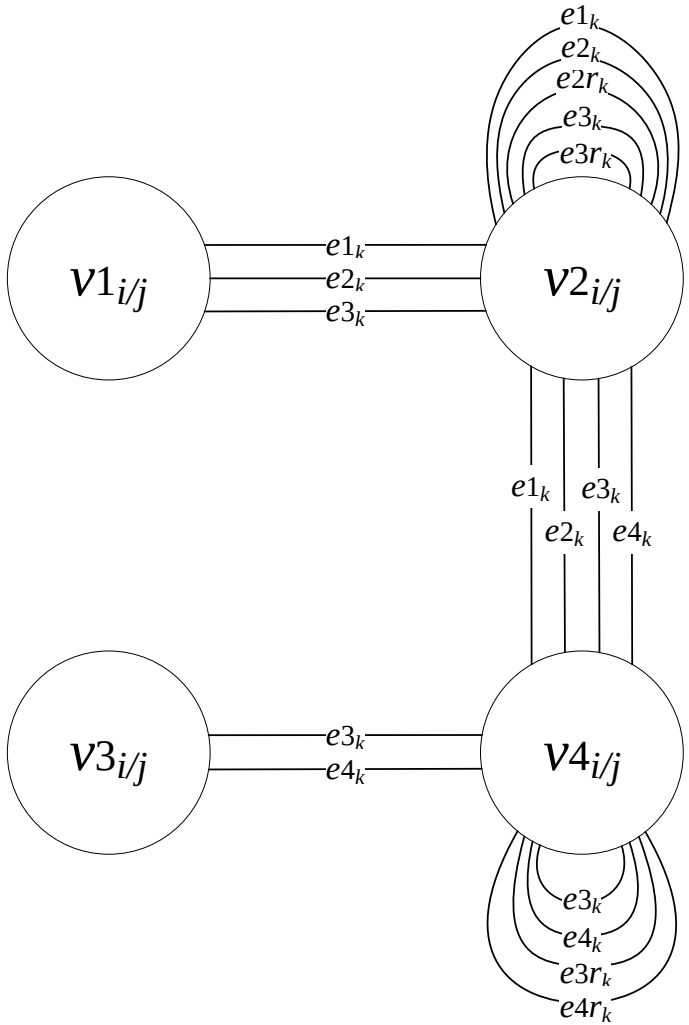
$E4r = \{e4r_1, e4r_2, e4r_3, \ldots, e4r_{m4r}\}$ – подмножество сред дистанционного распространения информации в киберпространстве.

# ПРИМЕРЫ САНКЦИОНИРОВАННЫХ СРЕД РАСПРОСТРАНЕНИЯ ИНФОРМАЦИИ

ТУСУР
TUSUR UNIVERSITY

| | $v1_i, v2_j / v2_i, v1_j$ | $v2_i, v2_j$ | $v2_i, v4_j / v4_i, v2_j$ | $v3_i, v4_j / v4_i, v3_j$ | $v4_i, v4_j$ |
|---|---|---|---|---|---|
| $e1_k$ | кабинет, архив | комната для переговоров | кабинет, архив, комната для переговоров | - | - |
| $e2_k$ | | | | | |
| $e2r_k$ | - | почтовое отправление | - | - | - |
| $e3_k$ | аналоговые устройства записи/ воспроизведения аудио и видео информации | аналоговый телефон | цифровые устройства ввода (микрофон, клавиатура) и вывода (колонки, монитор) информации | цифровые устройства хранения информации, контроллер-концентратор ввода-вывода (южный мост) | оперативная память, видеокарта, контроллер памяти |
| $e3r_k$ | - | телефонная сеть | - | - | кабельная сеть, беспроводная сеть |
| $e4_k$ | - | - | драйверы цифровых устройств ввода-вывода | драйверы баз данных, файловой системы, цифровых устройств хранения информации | средства межпроцессного взаимодействия |
| $e4r_k$ | - | - | - | - | драйверы сетевых протоколов |

# МОДЕЛЬ ИНФОРМАЦИОННЫХ ПОТОКОВ В ВИДЕ МУЛЬТИГРАФА

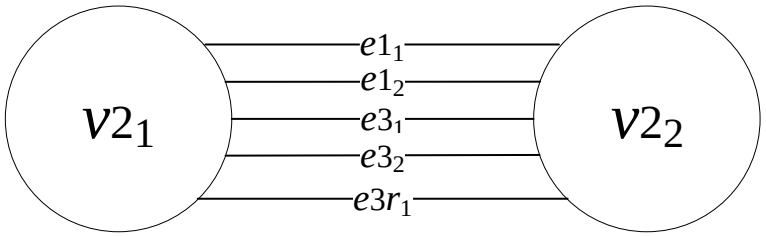



$F = \{f_1, f_2, f_3, f_4, f_5, f_6, f_7, f_8, f_9, f_{10}, f_{11}, f_{12}, f_{13}, f_{14}, f_{15}, f_{16}, f_{17}, f_{18}\}$, где $f_1 = (v1_i, e1_k, v2_j)$; $f_2 = (v1_i, e2_k, v2_j)$; $f_3 = (v1_i, e3_k, v2_j)$; $f_4 = (v2_i, e1_k, v2_j)$; $f_5 = (v2_i, e2_k, v2_j)$; $f_6 = (v2_i, e3_k, v2_j)$; $f_7 = (v2_i, e2r_k, v2_j)$; $f_8 = (v2_i, e3r_k, v2_j)$; $f_9 = (v2_i, e1_k, v4_j)$; $f_{10} = (v2_i, e2_k, v4_j)$; $f_{11} = (v2_i, e3_k, v4_j)$; $f_{12} = (v2_i, e4_k, v4_j)$; $f_{13} = (v3_i, e3_k, v4_j)$; $f_{14} = (v3_i, e4_k, v2_j)$; $f_{15} = (v4_i, e3_k, v4_j)$; $f_{16} = (v4_i, e3r_k, v4_j)$; $f_{17} = (v4_i, e4_k, v4_j)$; $f_{18} = (v4_i, e4r_k, v4_j)$.

На основе неориентированного мультиграфа можно выделить 18 типов элементарных информационных потоков, состоящих из троек «источник»–«среда распространения»–«приемник». При этом, *i*-е и *j*-е элементы могут принимать значение и источника, и приемника.

# ПРИМЕР. КОНФИДЕНЦИАЛЬНЫЙ РАЗГОВОР ПО ТЕЛЕФОНУ

ТУСУР
TUSUR UNIVERSITY




Элементы системы, реализующей телефонный разговор*:*

$V2 = \{v2_1, v2_2\}$,

где $v2_1$ – абонент №1, $v2_2$ – абонент №2.

$E1 = \{e1_1, e1_2\}$,

где $e1_1$ – кабинет №1 (санкционированная зона слышимости абонента №1), $e1_2$ – кабинет №2 (санкционированная зона слышимости абонента №2).

$E3 = \{e3_1, e3_2\}$,

где $e3_1$ – телефон №1 (принадлежит абоненту №1), $e3_2$ – телефон №2 (принадлежит абоненту №2).

$E3r = \{e3r_1\}$,

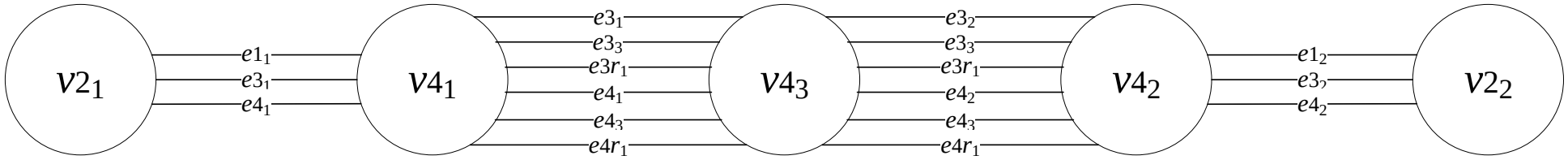
где $e3r_1$ – телефонная сеть.

Множество информационных потоков для телефонного разговора:

$F_{tp} = (v2_1, e1_1, v2_2), (v2_1, e1_2, v2_2), (v2_1, e3_1, v2_2), (v2_1, e3_2, v2_2), (v2_1, e3r_1, v2_2)$.

# ПРИМЕР. КОНФИДЕНЦИАЛЬНЫЙ РАЗГОВОР С ИСПОЛЬЗОВАНИЕМ IP-ТЕЛЕФОНИИ

ТУСУР
TUSUR UNIVERSITY




Элементы системы, реализующей телефонный разговор с использованием IP-телефонии:

$V2 = \{v2_1, v2_2\}$, где $v2_1$ – абонент №1, $v2_2$ – абонент №2.

$V4 = \{v4_1, v4_2, v4_3\}$, где $v4_1$ – прикладной процесс (программа), реализующий функции клиента на IP-телефоне №1, $v4_2$ – прикладной процесс, реализующий функции клиента на IP-телефоне №2, $v4_3$ – прикладной процесс, реализующий функции сервера IP-телефонии.

$E1 = \{e1_1, e1_2\}$, где $e1_1$ – кабинет №1 (санкционированная зона слышимости абонента №1), $e1_2$ – кабинет №2 (санкционированная зона слышимости абонента №2).

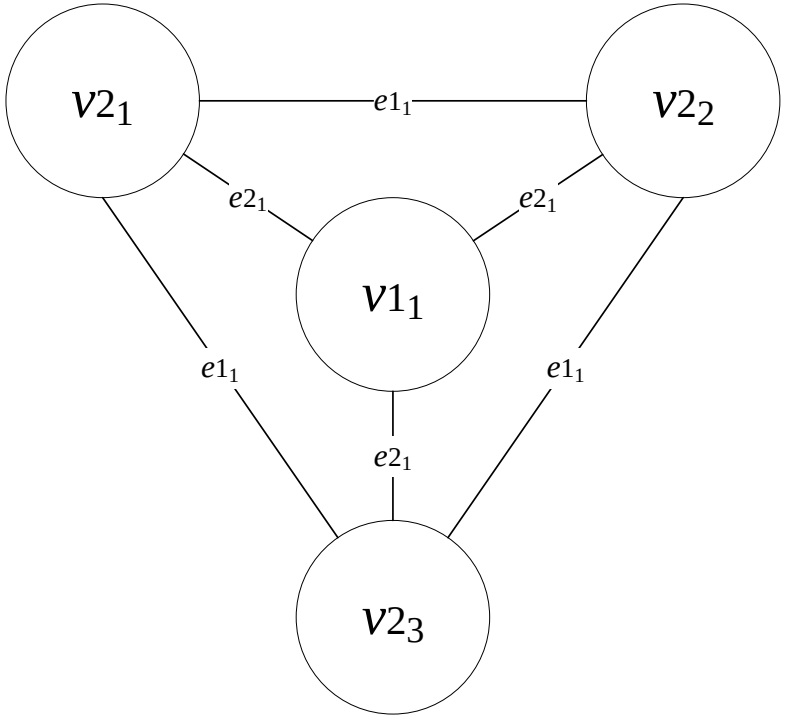
$E3 = \{e3_1, e3_2, e3_3\}$, где $e3_1$ – IP-телефон №1 (принадлежит абоненту №1), $e3_2$ – IP-телефон №2 (принадлежит абоненту №2), $e3_3$ – сервер IP-телефонии.

$E3r = \{e3r_1\}$, где $e3r_1$ – кабельная сеть на основе Ethernet.

$E4 = \{e4_1, e4_2, e4_3\}$, где $e4_1$ – операционная система IP-телефона №1, $e4_2$ – операционная система IP-телефона №2, $e4_3$ – операционная система сервера IP-телефонии.

$E4r = \{e4r_1\}$, где $e4r_1$ – стек протоколов IP-телефонии.

# ПРИМЕР. СОВЕЩАНИЕ РАБОЧЕЙ ГРУППЫ, СОСТОЯЩЕЙ ИЗ 3-Х ЧЕЛОВЕК




Элементы системы, реализующей совещание:

$V1 = \{v1_1\}$,

где $v1_1$ – конфиденциальный документ.

$V2 = \{v2_1, v2_2, v2_3\}$,

где $v2_1$ – сотрудник №1, $v2_2$ – сотрудник №2, $v2_3$ – сотрудник №3.

$E1 = \{e1_1\}$,

где $e1_1$ – помещение, разрешенное для проведения совещаний и переговоров (санкционированная зона слышимости).

$E2 = \{e2_1\}$,

где $e2_1$ – помещение, разрешенное для проведения совещаний и переговоров (санкционированная зона видимости).

Множество информационных потоков для проведения совещания:

$F_{mt} = (v1_1, e2_1, v2_1), (v1_1, e2_1, v2_2), (v1_1, e2_1, v2_3), (v2_1, e1_1, v2_2), (v2_1, e1_1, v2_3), (v2_2, e1_1, v2_3)$.

# МОДЕЛЬ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ ПОТОКОВ

ТУСУР
TUSUR UNIVERSITY

$$F \times TF = F \times (TFC \cup TFI) = (F \times TFC) \cup (F \times TFI),$$

где $TFC$ – модель угроз конфиденциальности информации,

$TFI$ – модель угроз целостности и доступности информации.

Множество типовых угроз конфиденциальности информации:

$$TFC = \{tfc_{11}, tfc_{12}, tfc_{21}, tfc_{22}, tfc_{31}, tfc_{32}\},$$

где $tfc_{11}$ – получение несанкционированным элементом $v_i$ информации, находящейся в санкционированной среде распространения;

$tfc_{12}$ – получение несанкционированным элементом $v_i$ информации, находящейся за пределами санкционированной среды распространения;

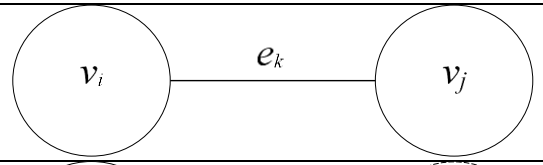
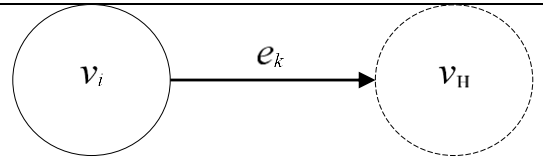
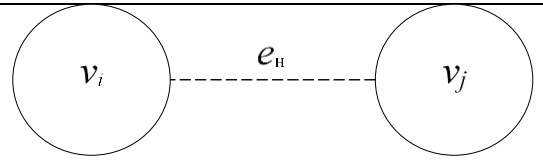
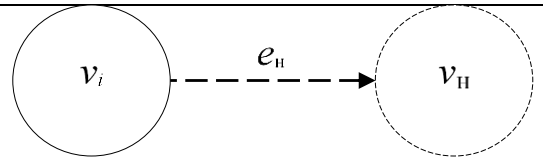
$tfc_{21}$ – получение несанкционированным элементом $v_j$ информации, находящейся в санкционированной среде распространения;

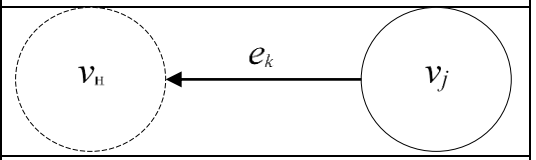
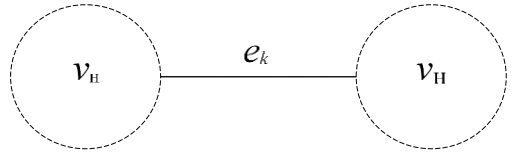
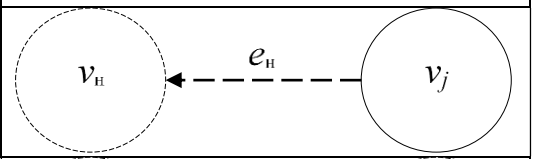
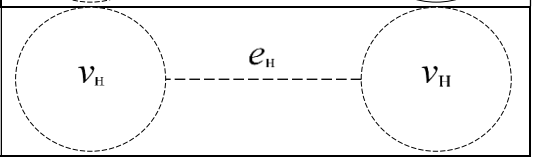
$tfc_{22}$ – получение несанкционированным элементом $v_j$ информации, находящейся за пределами санкционированной среды распространения;

$tfc_{31}$ – получение информации, находящейся в санкционированной среде распространения, злоумышленником, находящимся за ее пределами;

$tfc_{32}$ – получение информации за пределами санкционированной среды распространения $e_k$.

# СОСТОЯНИЯ ЭЛЕМЕНТАРНОГО ИНФОРМАЦИОННОГО ПОТОКА

| Обозначение состояния | Обозначение потока | Граф потока |
|---|---|---|
| $tfc_{31}$ | $v_i, e_k, v_j$ |  |
| $tfc_{21}$ | $v_i, e_k, v_н$ |  |
| $tfc_{32}$ | $v_i, e_н, v_j$ |  |
| $tfc_{22}$ | $v_i, e_н, v_н$ |  |

| Обозначение состояния | Обозначение потока | Граф потока |
|---|---|---|
| $tfc_{11}$ | $v_н, e_k, v_j$ |  |
| Нецелевое использование ресурсов (не рассматривается в качестве угрозы) | $v_н, e_k, v_н$ |  |
| $tfc_{12}$ | $v_н, e_н, v_j$ |  |
| Угроза отсутствует, т.к. отсутствуют санкционированные элементы | $v_н, e_н, v_н$ |  |

# ПРИМЕР. ПЕРЕЧЕНЬ УГРОЗ КОНФИДЕНЦИАЛЬНОСТИ ДЛЯ ИНФОРМАЦИОННОГО ПОТОКА $f_1 = (v1_i, e2_k, v2_j)$ – (документ, визуальный канал, человек)

ТУСУР
TUSUR UNIVERSITY

| | $tfc_{x1}$ | $tfc_{x2}$ |
|---|---|---|
| $tfc_{1x}$ | утечка из-за ознакомления злоумышленника с документом в санкц. помещении | н/с ознакомление с документом, вынесенным за пределы санкц. помещения (из-за кражи, утери и т.п.) |
| $tfc_{2x}$ | утечка информации из-за создания сотрудником н/с копии документа в санкц. помещении | утечка информации из-за н/с создания сотрудником новых носителей за пределами санкц. помещения |
| $tfc_{3x}$ | перехват информации по визуальному каналу во время работы с документом злоумышленником, находящимся за пределами санкц. помещения | утечка информации во время работы сотрудника с документом в н/с помещении (например, дома) |

# ПРИМЕР. ПЕРЕЧЕНЬ УГРОЗ КОНФИДЕНЦИАЛЬНОСТИ ДЛЯ ИНФОРМАЦИОННОГО ПОТОКА $f_1 = (v3_i, e3_k, v4_j)$ – (данные на диске/флешке, диск/флешка, процесс)

| | $tfc_{x1}$ | $tfc_{x2}$ |
|---|---|---|
| $tfc_{1x}$ | утечка информации из-за НСД к данным на санкц. устройстве хранения информации | утечка информации из-за наличия аппаратной закладки в используемом персональном компьютере |
| $tfc_{2x}$ | утечка из-за создания н/с копии данных на санкц. устройстве хранения | утечка информации из-за копирования данных на н/с устройство хранения |
| $tfc_{3x}$ | перехват ПЭМИН при работе с санкц. устройством хранения | утечка данных из-за подключения устройства хранения информации к н/с персональному компьютеру |

# ПРИМЕР. ПЕРЕЧЕНЬ УГРОЗ КОНФИДЕНЦИАЛЬНОСТИ ДЛЯ ИНФОРМАЦИОННОГО ПОТОКА $f_1 = (v3_i, e4_k, v4_j)$ – (файл, драйвер файловой системы, процесс)

ТУСУР
TUSUR UNIVERSITY

| | $tfc_{x1}$ | $tfc_{x2}$ |
|---|---|---|
| $tfc_{1x}$ | утечка информации из-за НСД к файлу в месте его санкц. хранения | утечка информации из-за наличия программной закладки в ОС |
| $tfc_{2x}$ | утечка информации из-за создания н/с копии файла на санкц. логическом диске | утечка информации из-за создания н/с копии файла на н/с логическом диске |
| $tfc_{3x}$ | считывание остаточной информации с логического диска после удаления файла | НСД к файлу из-за загрузки н/с ОС |

# КЛАССИФИКАЦИЯ УГРОЗ ЦЕЛОСТНОСТИ И ДОСТУПНОСТИ

ТУСУР
TUSUR UNIVERSITY

| | Носитель информации | Среда распространения |
|---|---|---|
| Н/с изменение | Внесение н/с корректировок, исправлений в файлы, записи БД | Помехи, ошибки считывания и т.п. |
| Н/с уничтожение | Н/с удаление файла, записи БД | Нарушение доступности по причине уничтожения драйверов, накопителей и т.п. |
| Подмена данных | Фальсификация данных, дезинформация | Нарушение доступности по причине отказа в обслуживании (подмена легальных данных на большое количество несанкционированных) |

# АТРИБУТИВНЫЙ МЕТАГРАФ

ТУСУР
TUSUR UNIVERSITY

Атрибутивный метаграф представляет собой упорядоченную четверку:

$$MG = (V, MV, E, ME),$$

где $MG$ – метаграф;

$V$ – множество вершин метаграфа;

$MV$ – множество метавершин метаграфа;

$E$ – множество ребер метаграфа;

$ME$ – множество метаребер метаграфа.

Вершина метаграфа характеризуется множеством атрибутов:

$$v_i = \{atr_k\},$$

где $v_i$– вершина метаграфа, $v_i \in V$;

$atr_k$ – атрибут.

Ребро метаграфа характеризуется множеством атрибутов, исходной и конечной вершиной, признаком направленности:

$$e_j = (V_s, V_E, eo, \{atr_k\}),$$

где $e_j$ – ребро метаграфа, $e_j \in E$;

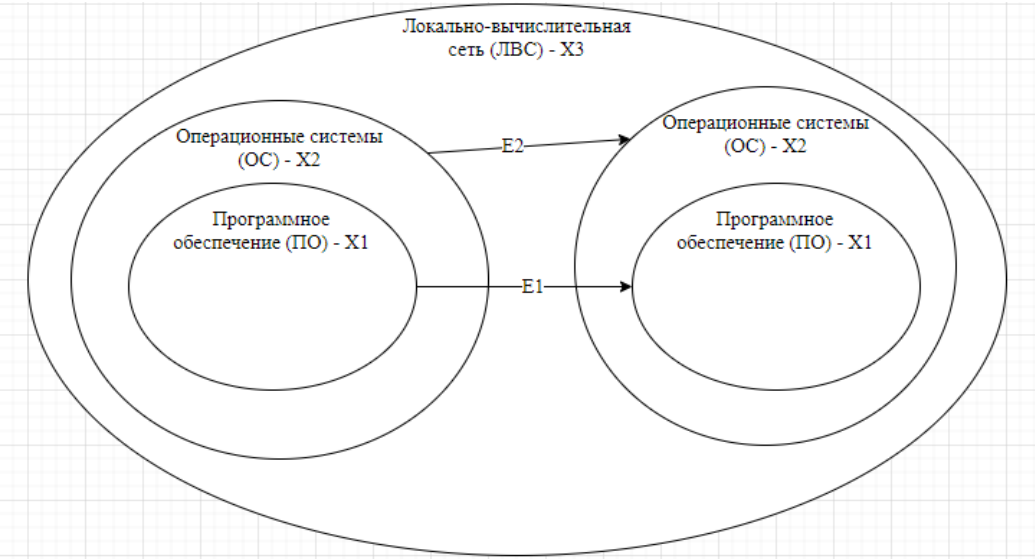
$V_s$ – исходная вершина (метавершина) ребра;

$V_E$ – конечная вершина (метавершина) ребра;

$eo$ – признак направленности ребра;

$atr_k$– атрибут.

# ПРИМЕР МЕТАГРАФА В РАМКАХ КИБЕРПРОСТРАНСТВА




Атрибутивный метаграф:

$$G = (X_1, X_2, X_3, E_1, E_2, E_3),$$

где $G$ – атрибутивный метаграф вложенности 3;

$X_1 = \{x_1^k\}$ , $k = \overline{1,q}$ – множество программного обеспечения;

$X_2 = \{x_2^l\}$, $l = \overline{1,r}$ – множество операционных систем, $x_2^l \subset X_1$;

$X_3 = \{x_3^m\}$, $m = \overline{1,s}$ – множество ЛВС, $x_3^m \subset X_2$;

$E_1 = \{e_1^n\}$ , $n = \overline{1,t}$ – множество связей между программным обеспечением, определенных на множестве $X_1$;

$E_2 = \{e_2^o\}$ , $o = \overline{1,u}$ – множество связей между операционными системами, определенных на множестве $X_2$;

$E_3 = \{e_3^p\}$, $p = \overline{1,v}$ – множество связей между локальными вычислительными сетями, определенных на множестве $X_3$.

# КЛАССИФИКАЦИЯ УГРОЗ ВЫЯВЛЕНИЯ УЯЗВИМОСТЕЙ СИСТЕМЫ

ТУСУР
TUSUR UNIVERSITY

1. Разглашение информации о местоположении элемента системы – IP-, MAC-адреса, номера кабинета с документами ограниченного доступа или серверной и т.п.
2. Разглашение информации о механизмах защиты – перечень средств защиты, списки доступа, ключи шифрования и т.п.
3. Разглашение информации о параметрах (атрибутах) элемента системы – открытые порты, тип и версия ОС, веб-сервера, драйвера и т.п.

# КЛАССИФИКАЦИЯ УГРОЗ НАРУШЕНИЯ АУТЕНТИЧНОСТИ СИСТЕМЫ

ТУСУР
TUSUR UNIVERSITY

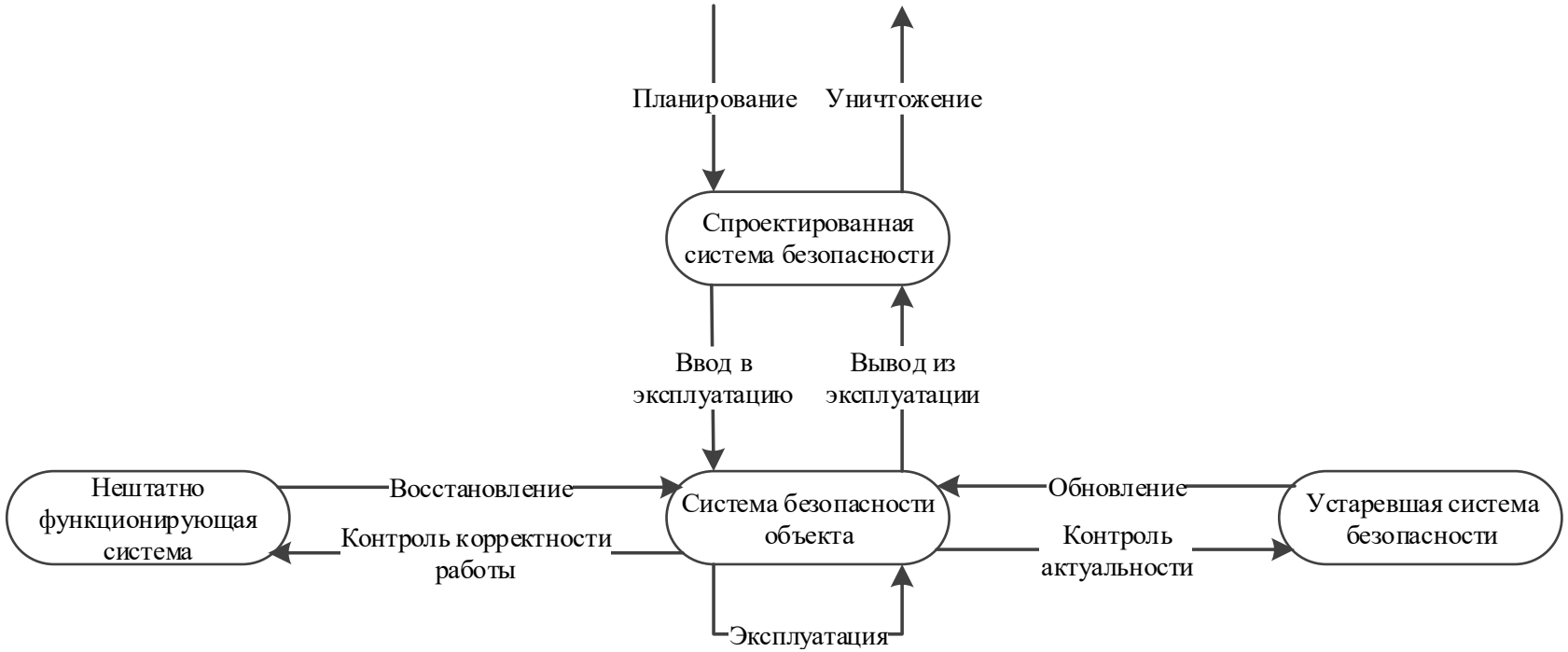
| Тип угрозы | Физическая среда | Виртуальная среда |
|---|---|---|
| Несанкционированный вывод из строя компонента, пользователя (учётной записи) или канала связи | Сбой системы электроснабжения<br>Несанкционированное отключение средств защиты (сигнализации и т.п.)<br>Кража оборудования или носителей информации<br>Вывод/выход из строя узлов ПЭВМ, структурированной кабельной сети | Отключение средств защиты (например, механизмов аудита, консолей оператора мониторинга)<br>Очистка/затирание истории команд и журналов регистрации<br>Отключение сервисов (веб-сервера, электронной почты и т.п.)<br>Несанкционированное удаление учётной записи |
| Внедрение несанкционированного компонента, пользователя или канала связи | Несанкционированное подключение внешних устройств<br>Дарение носителей информации (например, флэш), содержащих вредоносное программное обеспечение<br>Внедрение злоумышленника в структуру организации | Внедрение вредоносных программ (вирусов)<br>Установка ПО, не связанного с исполнением служебных обязанностей<br>Внедрение ложного объекта как в систему, так и во внешних сетях<br>Скрытая установка и запуск средств удаленного доступа<br>Выполнение кода через различного рода загрузчики, с помощью эксплоитов<br>Несанкционированное создание учетных записей |

# КЛАССИФИКАЦИЯ УГРОЗ НАРУШЕНИЯ АУТЕНТИЧНОСТИ СИСТЕМЫ

ТУСУР
TUSUR UNIVERSITY

| Тип угрозы | Физическая среда | Виртуальная среда |
|---|---|---|
| Подмена компонента, пользователя или канала связи | Маскирование подключенных устройств под легитимные (например, нанесение корпоративного логотипа, инвентарного номера, телефона службы поддержки) | Подмена доверенного объекта сети, навязывание ложного маршрута сети, фишинг, фарминг<br><br>Подмена дистрибутивов программ<br><br>Подмена прошивок или программного обеспечения BIOS<br><br>Вход под чужой учётной записью |
| Изменение режима работы (параметров) компонента, пользователя (учётной записи) или канала связи | Нарушение штатного режима функционирования оборудования автоматизированной системы управления и управляемого объекта и/или процесса<br><br>Изменение принципов работы сотрудника за счёт шантажа или подкупа | Внесение в конфигурацию атакуемой системы или сети изменений, с помощью которых становится возможен многократный запуск вредоносного кода<br><br>Внесение записей в реестр, автозагрузку, планировщики заданий, обеспечивающих запуск вредоносного программного обеспечения при перезагрузке системы или сети<br><br>Перехват управления загрузкой с изменением необходимой технологической информации для получения НСД в операционную среду информационной системы.<br><br>Изменение параметров функционирования средств защиты информации |

# МОДЕЛЬ ЖИЗНЕННОГО ЦИКЛА СИСТЕМЫ ЗАЩИТЫ ОБЪЕКТА ИНФОРМАТИЗАЦИИ




**Система защиты информации (СЗИ) –** совокупность органов и (или) исполнителей, используемой ими техники защиты информации, а также объектов защиты информации, организованная и функционирующая по правилам и нормам, установленным соответствующими документами в области защиты информации.

# КЛАССИФИКАЦИЯ УГРОЗ ЖИНЕННОГО ЦИКЛА ОБЪЕКТА ИНФОРМАТИЗАЦИИ

ТУСУР
TUSUR UNIVERSITY

1. Угрозы выявления уязвимостей в управлении компонентами объекта информатизации и его системы защиты

| Физическая среда | Виртуальная среда |
|---|---|
| Принципы работы охраны – порядок обхода здания, снятия и сдачи помещений под охрану и т.п. | Регламенты антивирусной защиты, работы со средствами аутентификации и т.п. |
| Чувствительная информация о сотрудниках, которую можно использовать для шантажа или подкупа | Пароли, ключи шифрования, которые используют сотрудники |
| Регламенты работы персонала с информацией ограниченного доступа | Регламенты работы персонала с защищаемой информацией в автоматизированных системах |

2. Угрозы нарушения доверия к объекту информатизации и его системе защиты

| Физическая среда | Виртуальная среда |
|---|---|
| Внедрение скрытых функций (закладок) в продукцию на этапе разработки, производства, поставки, эксплуатации, ремонта | Внедрение недекларированных возможностей в системное и прикладное ПО |
| Несоответствие регламентов действующему законодательству | Ошибки при разработке ПО и средств защиты информации |

# МЕТОДОЛОГИЯ КЛАССИФИКАЦИИ УГРОЗ

ТУСУР
TUSUR UNIVERSITY

| | | | |
|---|---|---|---|
| *Метод функционального моделирования на основе IDEF0* | Методика определения объектов защиты (информация и ее носители – горизонтальные стрелки) | Методика определения объектов защиты (компоненты системы – стрелки снизу) | Методика определения объектов защиты (компоненты управления – стрелки сверху) |
| *Метод структурного моделирования на основе теории графов* | Модель информационных потоков | Модель объекта информатизации | Модель жизненного цикла системы защиты информации |
| *Классификация угроз информационной безопасности* | Модель угроз конфиденциальности информации | Модель угроз выявления уязвимостей системы | Модель угроз выявления уязвимостей при управлении системой |
| | Модель угроз целостности и доступности информации | Модель угроз нарушения аутентичности системы | Модель угроз нарушения доверия к системе |

# ОБОБЩЕННАЯ МОДЕЛЬ УГРОЗ

ТУСУР
TUSUR UNIVERSITY

$$T = (F \times TF) \cup (S \times TS) \cup (M \times TM),$$

где $F$ – модель информационных потоков,

$S$ – модель объекта информатизации,

$M$ – модель жизненного цикла объекта информатизации,

$TF$ – множество типовых угроз безопасности информационных потоков,

$TS$ – множество типовых угроз безопасности объекта информатизации,

$TM$ – множество типовых угроз безопасности жизненного цикла объекта информатизации.

# ТИПОВЫЕ УГРОЗЫ БЕЗОПАСНОСТИ ИНФОРМАЦИИ

ТУСУР
TUSUR UNIVERSITY

| *Угрозы, связанные с носителем информации* | *Угрозы, связанные со средой распространения информации* |
|---|---|
| **Класс «Угрозы конфиденциальности информации»** | |
| Несанкционированное получение информации с носителя в санкционированной среде распространения | Контроль санкционированной среды распространения |
| Несанкционированное получение информации с носителя за пределами санкционированной среды распространения | Перехват информации за пределами санкционированной среды распространения |
| Запись информации на несанкционированный носитель в санкционированной среде распространения | |
| Запись информации на несанкционированный носитель за пределами санкционированной среды распространения | |
| **Класс «Угрозы целостности информации»** | |
| Искажение информации на носителе | Искажение информации при передаче в среде распространения |
| Подмена (фальсификация) информации на носителе | |
| Уничтожение информации на носителе | |
| Уничтожение информации вместе с носителем | |
| **Класс «Угрозы доступности информации»** | |
| | Отказ в обслуживании из-за подмены информации в среде распространения |
| | Блокирование передачи информации в среде распространения |
| | Невозможность передачи информации из-за неработоспособности среды распространения |

# ТИПОВЫЕ УГРОЗЫ БЕЗОПАСНОСТИ

ТУСУР
TUSUR UNIVERSITY

Типовые угрозы безопасности компонентам системы

| **Класс «Угрозы нарушения аутентичности системы»** | **Класс «Угрозы выявления уязвимостей системы»** |
|---|---|
| Несанкционированная подмена компонента системы | Утечка информации о имени/адресе компонента системы |
| Выход из строя санкционированного компонента системы | |
| Добавление несанкционированного компонента системы | |
| Несанкционированное изменение параметров компонента системы | Утечка информации о параметрах (режимах работы) компонента системы |

Типовые угрозы, возникающие на этапах жизненного цикла системы защиты

| **Класс «Угрозы выявления уязвимостей при управлении системой»** | **Класс «Угрозы нарушения доверия к системе»** |
|---|---|
| Выявление уязвимости из-за случайных или преднамеренных нарушений правил управления жизненным циклом системы | Появление уязвимости из-за случайных или преднамеренных нарушений правил управления жизненным циклом системы |

# ПРЕИМУЩЕСТВА ПРИМЕНЕНИЯ МЕТОДОЛОГИИ

ТУСУР
TUSUR UNIVERSITY

- Основная работа эксперта – построение модели объекта защиты, а не формулирование угроз). Как следствие, уменьшение субъективности и получение более качественного перечня угроз.
- Формализация описания объектов защиты, включая разделение на носители информации и компоненты, предназначенные для распространения информации.
- Учёт угроз в физических средах, а не только в киберпространстве.
- Классификация угроз обладает полнотой.

# Thank you!

Questions?

Contact: kaa@fb.tusur.ru